

5

encrypting the created set of N trap door, the encryption-decryption function pairs and the randomly

[illegible]

selected trap door function along with the decryption key prior to recording in an escrow database.

3. The method for withdrawing an encryption key from a key escrow database as in Claim 1, further
5 comprising:

randomly selecting at the receiver an additional trap door encryption-decryption function pair and the paired token;

adding randomization information to the additional
10 selected trap door encryption-decryption function pair and the corresponding token;

concatenating the results of the adding of randomization information to the additional selected trap door encryption-decryption function pair to the
15 encryption of the randomly selected first trap door encryption-decryption function pair; and

encrypting the concatenating results using the encryption key from the second choice.

4. The method for withdrawing an encryption key
20 from a key escrow database as in Claim 1 further comprising adding signature information to the selected trap door encryption-decryption function pair to distinguish valid subsequent decodings from invalid decodings.

5. The method for withdrawing an encryption key
25 from a key escrow database as in Claim 1, wherein encrypting a selected trap door encryption-decryption function pair comprises calculating a cryptogram utilizing the corresponding token and including an
30 encryption key along with randomization information, as

ATTORNEY'S DOCKET
064751.0298

PATENT APPLICATION

88

well as additional information added for signature
purposes.

064751.0298

generating, in accordance with a selected encryption
function, a set of N cryptogram/decryption key pairs,
5 each pair having a corresponding token;

randomly selecting at the receiver one of the
cryptogram/decryption key pairs along with the
10 corresponding token;

generating a cryptogram utilizing the corresponding
15 encryption key and comprising the selected token and
randomization information;

inverting the recorded set of N cryptogram/decryption key pairs and the generated cryptogram to identify an encryption key from the key escrow database.

randomly selecting at the receiver one or more additional N cryptogram/decryption key pairs and corresponding tokens;

30 decrypting each cryptogram using the associated
token of the additionally selected encryption/decryption

generating a response/cryptogram for each additionally selected cryptogram/decryption key pair
5 utilizing the corresponding encryption key and comprising the selected token and randomization information; and

8. The method for withdrawing encryption keys from a key escrow database as in Claim 6, further comprising:

9. The method for withdrawing encryption keys from a key escrow database as in Claim 8 wherein mixing comprises utilization of a linear transform.

11. The method for withdrawing encryption keys from a key escrow database as in Claim 8 wherein mixing further comprises utilization of a public key cryptosystem.

12. The method for withdrawing encryption keys from a key escrow database as in Claim 6 wherein recording in an escrow database further comprises encrypting the generated set of N cryptogram decryption key pairs and the response message prior to recording.

5

[illegible]

creating at an originator a set of N trap door
5 functions each paired with a corresponding token, each
trap door function comprising a cryptogram/decryption key
pair;

10 randomly selecting at the receiver one of the trap
door functions and the paired token;

```

    encrypting an escrow/key with the randomly selected
15 trap door function;

```

decoding the encrypted escrow key with the randomly
selected trap door function utilizing retained trap door
20 information.

25 16. The method as in Claim 15 wherein encrypting an
escrow key comprises generating a cryptogram comprising
the corresponding token, the decryption key and
randomization information.

17. The method of Claim 14 wherein decoding the
30 encrypted key comprises selecting a decryption key
randomly from a selected group of decryption keys.

18. The method of Claim 17 further comprising recognizing a correct decoding result utilizing structural information embedded in the response message.

19. The method of Claim 14 wherein creating at an
5 originator further comprises generating the set of N trap door functions utilizing a selected encryption function and a private encryption key.

Add
a3

Add
B2

007260 92089960